# A Sieve Method for Factoring Numbers of the Form $n^2 + 1$

By Daniel Shanks

**1. Introduction.** Factorizations of numbers of the form $n^2 + 1$, [1], [2], are of mathematical interest for at least four reasons: 1) a possible insight into the unsettled question as to whether there are infinitely many primes of this form; 2) a possible insight into the unsettled question as to whether the reducible numbers (explained below) have a definite density; 3) the relation of these factorizations to the $p$-adic square roots of $-1$; and 4) the relation of these factorizations to the Gaussian primes. The purpose of this paper is to describe a sieve method for factoring these numbers and to present and discuss some empirical results bearing on 1), 2), 3), and 4) which were obtained by its use. The method can be considered to be based, in part, on the $p$-adic square roots of $-1$, but it is also possible to avoid the use of this language.

A program based on this sieve method was written for an IBM 704 with a 32,768-word high-speed memory, and with this program all $n^2 + 1$ from $n = 1$ to 180,000 were completely factored in about 10 minutes. Since these factorizations of $n^2 + 1$ exceed those in existing published tables, (82 percent of these numbers are greater than a billion), a short summarizing statistical table should be of interest. In the table below, $P(N)$ is the number of primes of the form $n^2 + 1$ for $1 \leqq n \leqq N$, and for comparison, $\pi_-(N)$ is the number of primes of the form $4m - 1$ for $1 < 4m - 1 \leqq N$. Further, $R(N)$ is the number of reducible numbers $\leqq N$, $r(N) = R(N) - R(N - 10{,}000)$, and $\delta_R(N) = R(N)/N$, the *mean* density of the reducibles.

Statistical Table of Primes and Reducibles

| $N$ | $r(N)$ | $R(N)$ | $\delta_R(N)$ | $P(N)$ | $\pi_-(N)$ | $P(N)/\pi_-(N)$ |
|---|---|---|---|---|---|---|
| 10,000 | 2898 | 2898 | .28980 | 841 | 619 | 1.3586 |
| 20,000 | 2935 | 5833 | .29165 | 1559 | 1136 | 1.3724 |
| 30,000 | 2930 | 8763 | .29210 | 2268 | 1633 | 1.3889 |
| 40,000 | 2918 | 11681 | .29203 | 2952 | 2117 | 1.3944 |
| 50,000 | 2959 | 14640 | .29280 | 3613 | 2583 | 1.3988 |
| 60,000 | 2912 | 17552 | .29253 | 4252 | 3038 | 1.3996 |
| 70,000 | 2965 | 20517 | .29310 | 4888 | 3485 | 1.4026 |
| 80,000 | 2881 | 23398 | .29248 | 5513 | 3933 | 1.4017 |
| 90,000 | 2947 | 26345 | .29272 | 6084 | 4364 | 1.3941 |
| 100,000 | 2875 | 29220 | .29220 | 6656 | 4808 | 1.3844 |
| 110,000 | 3009 | 32229 | .29299 | 7239 | 5247 | 1.3796 |
| 120,000 | 2934 | 35163 | .29303 | 7795 | 5675 | 1.3736 |
| 130,000 | 2938 | 38101 | .29308 | 8369 | 6103 | 1.3713 |
| 140,000 | 2888 | 40989 | .29278 | 8944 | 6531 | 1.3695 |
| 150,000 | 2983 | 43972 | .29315 | 9505 | 6941 | 1.3694 |
| 160,000 | 2952 | 46924 | .29328 | 10072 | 7361 | 1.3683 |
| 170,000 | 2932 | 49856 | .29327 | 10658 | 7770 | 1.3717 |
| 180,000 | 2981 | 52837 | .29354 | 11223 | 8178 | 1.3723 |

Received March 10, 1959.

**2. The Sieve.** The sieve method (substantially more complicated than that of Eratosthenes) is based on the facts listed in the following theorem. Since many of these are well known and the rest can be easily verified, no proof need be given.

THEOREM. For every prime $p$ of the form $4m + 1$ and every positive integer $k$ there are two and only two positive solutions of:

$$\begin{cases} n < p^k \\ n^2 + 1 \equiv 0 \pmod{p^k}. \end{cases} \tag{1}$$

If we call these $A_k$ and $B_k$, then

$$A_k + B_k = p^k, \tag{2}$$

and if

$$h \equiv \tfrac{1}{2}(p + 1)A_1 \pmod{p}, \tag{3}$$

and

$$C_k \equiv h(A_k^2 + 1)/p^k \pmod{p}, \tag{4}$$

the $A_k$ for $k = 2, 3, \cdots$ may be computed recursively from $A_1$ by

$$A_{k+1} = A_k + C_k p^k. \tag{5}$$

Further, for all positive $n$,

$$n^2 + 1 \equiv 0 \pmod{p^k},$$

if and only if $n$ is given by one of the *linear* forms:

$$n = \begin{cases} A_k + mp^k \\ B_k + mp^k \end{cases} \qquad (m = 0, 1, 2, \cdots), \tag{6}$$

and aside from these factors of $n^2 + 1$ (obtained as $p$ runs through all primes of the form $4m + 1$) the only other prime-power factors are the obvious

$$n^2 + 1 \equiv 0 \pmod{2} \quad \text{for } n \equiv 1 \pmod{2}. \tag{7}$$

We will adopt the convention that $A_1$ is the *smaller* of the two roots of (1) for $k = 1$, and note that this implies:

$$A_1 < \tfrac{1}{2}p < B_1, \tag{8}$$

but it does *not* imply that $A_k < B_k$ if $k > 1$. For example, let $p = 5$. Then $A_1 = 2$. Thus $h = 1$, and for $k = 1, 2, 3, \cdots$ we compute:

$$A_k = 2, 7, 57, 182, 2057, 14557, \cdots$$

$$B_k = 3, 18, 68, 443, 1068, 1068, \cdots$$

and note, $A_5 > B_5$.

We also have in this case the interesting *degeneracy* $B_5 = B_6$. While similarly, for $p = 13$, we have the degeneracy $A_3 = A_4$, it can be seen from (1), and it is important for the validity of the sieve method, that for every $p$:

$$\begin{cases} A_1 < A_2 \\ B_1 < B_2. \end{cases} \tag{9}$$

Now suppose we wish to factor every $n^2 + 1$ for $1 \leqq n \leqq L$. The sieve method proceeds as follows:

A.) In $L$ contiguous cells we write the corresponding values of $n^2 + 1$.

B.) We now divide out the factor of 2 for each $n = 2m + 1$, $(m = 1, 2, \cdots)$ and store the quotients back into the same cells.

C.) At $n = 2$, we find the number 5. This implies (see a general proof below) that 5 is a $p$ and, corresponding to it, $A_1 = 2$. Using formulas (2) through (6), we factor a 5 from each $n$'th cell, where

$$n = \begin{cases} 2 + m5 & (m = 1, 2, \cdots) \\ 3 + m5 & (m = 0, 1, 2, \cdots) \end{cases}$$

and store back the quotients. Then a second 5 is factored for each

$$n = \begin{cases} 7 + m25 \\ 18 + m25 \end{cases} \qquad (m = 0, 1, 2, \cdots)$$

and so on until both $A_k$ and $B_k$ are greater than $L$. By now all factors of 5 have been removed.

D.) At $n = 3$, we now find the quotient 1. This means 3 is not an $A_1$ number. It is, in fact, reducible (see below). We so record it and move on.

E.) At $n = 4$, we find 17 and divide out all factors of 17 as in $C$.

F.) At $n = 5$, we find 13 and divide out all factors of 13.

G.) Proceeding in this way we examine the contents of the $n$'th cell when we get to it, and find one of two cases.

1. The quotient is 1 and no *new* prime factor is contained in $n^2 + 1$.

2. The quotient is $>1$. In this case the quotient must be a new $p = 4m + 1$ and $n$ must be its corresponding $A_1$ number. Proof: Since the quotient cannot have a factor of 2 or a prime of the form $4m - 1$, every prime factor must be a $p = 4m + 1$. But for such a $p$, $n$ must be $A_1$, for, if $p$ had occurred in an earlier $n^2 + 1$, its $A_1$ would have been encountered earlier and $p$ would have been factored out. By (9), $n^2 + 1$ is not divisible by $p^2$. Nor can $n$ be simultaneously an $A_1$ for two distinct primes, since from (8) the quotient:

$$(A_1^2 + 1)/p \leqq \tfrac{1}{2}A_1,$$

and therefore cannot contain a second prime which (again by (8)) must be $>2A_1$.

This completes the proof, and shows we are obtaining complete factorizations without the use of any trial divisions and without the need to know in advance the primes of the form $4m + 1$. They are, in fact, being generated (though not in numerical order) by the process itself.

**3. The Program.** In the 704 program mentioned above the following changes were desirable or expedient.

a.) The sieve was started with $-(n^2 + 1)$ in the $n$'th cell and the *absolute value* of each quotient was stored back in. If no division occurred in a particular cell the contents of this cell remained negative and this indicated that $n^2 + 1$ was a prime.

b.) Since in a binary machine division by 2 is so simple, step B was combined with step A.

c.) The factoring out of any prime $p$ began when $n$ reached its $B_1$ instead of its $A_1$. This saves time and memory and is equally valid.

d.) The linear forms, (6), are easily obtained by use of an index register. The high efficiency of this method makes possible over 3000 divisions/sec.

e.) The sieve is done in several segments. In a memory of 32,768 words, with 4096 words reserved for an operating routine, a sieve segment of 20,000 words is possible, since nearly 7000 words (see g) must be reserved to save the primes (and corresponding $A_1$ numbers) for later phases. The program itself, although quite intricate, takes less than 300 words.

f.) An upper limit, $L$, of 180,000 (9 segments) was chosen since a tenth segment would cause $n^2 + 1$ to overflow the length of a 704 word. This is $2^{35}$ (nearly 34.36 billion). Of course $n$ could be made larger by using double precision.

g.) Although 127,162 of the 180,000 numbers are $A_1$ numbers, in most cases the corresponding $p$ is enormous and is not used in sieving—the criterion being $p + A_1 \leqq L$. The number of $p$'s actually used was 6693.

h.) The program was checked by being repeated with a segment of 20,500. This changed all the phase relations in the linear forms (6). It also raised $L$ to 184,500 and we find $P(184{,}500) = 11{,}486$; $R(184{,}500) = 54{,}162$.

i.) If it were not for the "degeneracies" mentioned just before (9), a much simpler sieve method would be possible. One would *not* compute the $A_k$ and $B_k$ sequences and take out *all* factors of $p$ at *once* but could instead re-factor the $A_2 + mp^2$, the $B_2 + mp^2$, the $A_3 + mp^3$, etc., *when* $n$ came to $A_2$, $B_2$, $A_3$, etc., respectively. This was in fact attempted, and some very rare errors ensued. For example, one found $R(20{,}000) = 5832$ instead of the true 5833, the single error stemming from the degeneracy $B_5 = B_6$ (for $p = 5$) mentioned above.

j.) The main output of the program as described was the table shown above but in a much greater detail (the interval in $N$ being 100 instead of 10,000). The program actually computed $\pi_+(N)$ by counting the $p$'s instead of the $\pi_-(N)$ shown. A small modification of the program also produced a 360-page table showing the largest prime factor in every $n^2 + 1$ for $n = 1\ (1)\ 180{,}000$. Small auxiliary tables concerning the $p$-adic square roots (the $A_k$ and $B_k$ sequences above) and the distribution of the reducible numbers were also produced.

**4. The Primes.** Now consider $P(N)$ in the statistical table. We see a steady growth which is nearly proportional to $\pi_-(N)$. Since

$$\pi_-(N) \sim \frac{1}{2}\int_2^N \frac{dx}{\ln x}$$

by the prime number theorem, the numbers $P(N)$ are in excellent agreement with the conjectured formula [3] of Hardy and Littlewood:

$$P(N) \sim 0.68641 \int_2^N \frac{dx}{\ln x} \tag{10}$$

which therefore implies $P(N)/\pi_-(N) \sim 1.3728$.

The constant in (10) is equal to the infinite product, taken over all odd primes,

$$\frac{1}{2}\prod_{p=3}^{\infty}\left[1-\left(\frac{-1}{p}\right)(p-1)^{-1}\right],$$

where $(-1/p)$ is the Legendre symbol. It was computed by A. E. Western [4] who also verified the substantial correctness of (10) to $N = 15{,}000$. Since the infinite product converges too slowly, Western used a transformation of the product due to Littlewood. The following related formula is simpler:

$$\text{(10a)} \qquad 0.68641\cdots = \frac{3}{4}\frac{\zeta(6)}{G\zeta(3)}\prod_{p=4m+1}\left(1+\frac{2}{p^3-1}\right)\left(1-\frac{2}{p(p-1)^2}\right).$$

Here $G$ is Catalan's constant, and the product is taken over the $\pi_+$ primes. More rapid convergence may be obtained by multiplying through by the identity:

$$\text{(10b)} \qquad 1 = \left[\frac{17}{16}\frac{\zeta(8)}{L(4)\zeta(4)}\prod_{p=4m+1}\left(1+\frac{2}{p^4-1}\right)\right]^2$$

where $L(4) = \sum_0^\infty (-1)^n (2n+1)^{-4}$. With this improvement, the first two $p$'s, i.e., 5 and 13, already suffice to yield the five decimal places shown.

Among the *Gaussian integers*, $a + bi$, the Gaussian primes on the positive real axis are those of the form $4m - 1$, and thus are those counted by $\pi_-(N)$. On the other hand, $n + i$ is a Gaussian prime if and only if $n^2 + 1$ is a rational prime. Therefore, the column headed "$P(N)/\pi_-(N)$" shows that the $+1$ horizontal line in the Gauss plane (and therefore also the $-1$) has about a 37 percent greater density of primes than the axis has. (For an attractive picture of these primes see van der Pol's Tea Cloth, [5].)

It is of interest to mention briefly the "Gaussian twin" primes, i.e., those where $(n-1)^2 + 1$ and $(n+1)^2 + 1$ are both prime. They are not at all rare. In the last block of 1000 numbers with $L = 184{,}500$, we find no less than 9 pairs, namely: $n =$ 183585; 183635; 183685; 184055; 184075; 184145; 184185; 184325; and 184495. The last pair, 34038036037 and 34038774017, were the largest primes obtained by this program. The conjecture suggests itself that there are infinitely many such "twins."

It may also be mentioned that (although they were not particularly sought) the program yielded a very large collection of "large" primes, i.e., those over 10 digits. Not only are 4830 of the $n^2 + 1$ "large" primes, but many others are equal to twice a "large" prime. For example, $184499^2 + 1 = 2\cdot 17019940501$.

**5. The Reducible and Irreducible Numbers.** A *reducible* number, $r$, is a positive integer whose arctangent is a linear combination, with integer coefficients, of the arctangents of smaller positive integers:

$$\text{(11)} \qquad \tan^{-1} r = \sum_{n=1}^{r-1} a_n \tan^{-1} n.$$

If no such linear combination is possible, the number is *irreducible* [6]. For example, since

$$\tan^{-1} 3 = 3\tan^{-1} 1 - \tan^{-1} 2,$$

3 is reducible. So are 7 and 8, while 1, 2, 4, 5, 6, 9, and 10 are irreducible. (If we replace the arctangent function in (11) with the logarithm, we would be defining composites and primes instead, so that the irreducibles can be thought of as the quadratic analogue of the primes.) John Todd showed [6] that $r$ is reducible if and only if the greatest prime factor of $r^2 + 1$ is less than $2r$. For each irreducible, $n$, (other than 1), there is thus a unique prime $p > 2n$ which is the greatest prime factor of $n^2 + 1$. [6, p. 526]; and this is the $1 - 1$ correspondence indicated above between $A_1$ and $p$. $A_1$ numbers are therefore irreducible, and all others except 1 are reducible. This includes all $A_2$, $A_3$, $\cdots$, all $B_1$, $B_2$, $\cdots$, and some numbers, such as 21, which are neither $A_k$ nor $B_k$.

**6. The Density of Reducibles (Heuristic).** If $R(N)$ is the number of reducibles $\leqq N$, and $\delta_R(N) = R(N)/N$, and *if* $\text{Lim}_{N\to\infty} \delta_R(N)$ exists, we call this limit the density of the reducible numbers, and write it $\delta_R$.

$$\delta_R = \text{Lim}_{N\to\infty} R(N)/N, \quad \text{if it exists.} \tag{12}$$

However, its existence is still unsettled, as is the older, and somewhat related question:

$$\text{Does } P(N) \to \infty\,? \tag{13}$$

Early counts of the reducible numbers up to 5000, by J. C. P. Miller and Todd, [6], [7], [8], were based on Todd's criterion [6] and Wrench's table [2], and indicated that $\delta_R(N)$ persisted in the vicinity of 0.29. The present paper extends $N$ to 184,500 and shows a continuance of this state of affairs with a slow growth (in the mean) to about 0.293.

Chowla and Todd [7] have proved that if $C(N)$ is the number of numbers $n \leqq N$ for which the greatest prime factor of $n$ is greater than $2\sqrt{n}$, then the $\text{Lim}_{N\to\infty} C(N)/N$ exists and equals $\ln 2 = 0.693\cdots$. But note that here $n$ ranges through *all* numbers, not just those of the form $m^2 + 1$. *If* this latter class of numbers constituted a *good sample* of all the numbers as regards *factorization* properties, (with a rigorous definition!) it would follow from $2\sqrt{m^2 + 1} \sim 2m$ and Todd's criterion of reducibility that $\delta_R$ does exist and is equal to $1 - \ln 2 = 0.30685\cdots$.

But, if such a deduction were possible, it would probably also follow from the same line of reasoning (good sample concept) that the mean *local* density of primes of the form $m^2 + 1$, like that of the ordinary prime sequence, would be

$$\frac{1}{\ln (m^2 + 1)} \sim \frac{1}{2 \ln m}$$

and thus

$$P(N) \sim \frac{1}{2} \int_2^N \frac{dm}{\ln m} \sim \pi_-(N).$$

Now in fact we have seen that $P(N)$ remains persistently and significantly higher. And this greater prevalence of primes is consistent with the smaller fraction of reducibles (.293 instead of .307) which is observed. It is, of course, not precluded that $\delta_R(N)$ will rise to .307 for *very* much larger $N$. Its slow growth, mentioned above, seems to be of order of $a/\ln N$ and to be associated with the falling off in the mean local density of the excess primes, $P(N) - \pi_{-}(N)$. This (average) increase of $\delta_R(N)$ hardly shows in the Table since $\ln N$ changes so slowly and the fluctuations are almost of the same size. Nonetheless it is there and may carry $\delta_R(N)$ *nearly* up to 0.307.

The gross facts on which any attempted assessment of the "good sample" concept must be based are these. The $n^2 + 1$ numbers have only about $\frac{1}{2}$ of all primes, [9], as possible factors, but in "compensation" these factors occur twice as often (see (6) above). While this may suggest a factorability of the same order of magnitude, certainly no more exact equivalence is implied.

Assuming the future establishment of $R(N) \sim \delta_R \cdot N$, the (deeper?) question of $O(R(N) - \delta_R \cdot N)$ will arise. Concerning this question—that of the *uniformity* of the distribution of the reducibles—the following table and figure are informative. Each of the 1800 intervals of 100 numbers:

$$100m < n \leqq 100(m + 1) \qquad (m = 0, 1, \cdots, 1799)$$

has at least 17 reducible numbers and at most 42. The 52,837 reducibles $\leqq$ 180,000 are distributed as follows:

| $r$, no. of reducibles | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\nu$, no. of intervals | 5 | 6 | 5 | 13 | 22 | 29 | 69 | 82 | 93 | 127 | 154 | 147 | 167 |

| 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 179 | 140 | 147 | 130 | 93 | 72 | 41 | 31 | 16 | 16 | 11 | 1 | 4 |

In the Figure a bar graph of this distribution is compared with a binomial distribution, $\nu\ (r)$:

$$\nu = 1800 \frac{100!}{r!(100 - r)!} (0.2935)^r (0.7065)^{100-r} \tag{14}$$

where the "probability," 0.2935, was taken to be the final value of the mean density, $\delta_R(180{,}000)$.

**7. P-adic Numbers and Degeneracy.** The sequence of the partial sums of the infinite series:

$$A_1 + \sum_{k=1}^{\infty} C_k p^k, \tag{15}$$

where $p$ is a prime of the form $4m + 1$ and $A_1$ and the $C_k$ are determined by (1) through (4), is a *convergent* sequence in the *p-adic sense.* (See [10] for an elementary account of $p$-adic valuation.) Since it converges, it represents a $p$-adic number, namely, one of the two values of $\sqrt{-1}$. This sequence, it is seen from (5), is the sequence $A_k$. The other sequence, $B_k$, converges in the $p$-adic sense to the other $\sqrt{-1}$ and their sum, $A_k + B_k$, converges in the $p$-adic sense to 0.

As an example, take $p = 5$, and $A_k = 2, 7, 57, 182$, etc., as above. If we write them in the quinary system we see that they represent the sequence obtained from the 5-adic number

$$\cdots 3140223032431212. = \sqrt{-1} \tag{16}$$

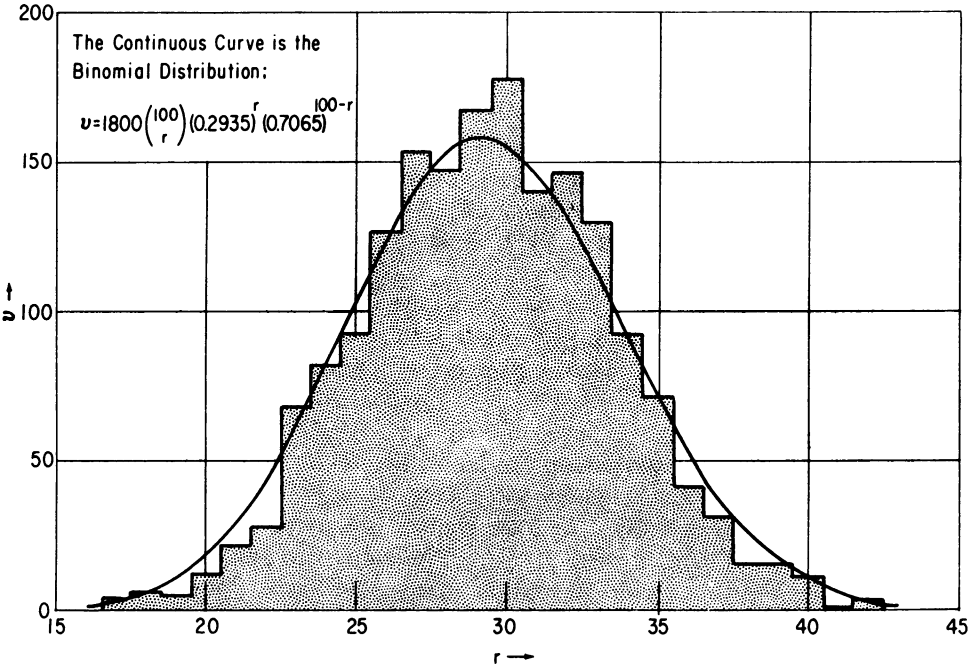

FIG. 1.—Distribution of the reducible numbers between 1 and 180,000 into the 1800 intervals of 100.

by starting at the quinary point and taking more and more places *to the left.* If we take $k$ places and carry the computation to at least $k$ places we find that

$$A_k^2 + 1 = \underbrace{\cdots\cdot 000 \cdots 00.}_{k \text{ zeroes}}$$

so that $A_k^2 + 1$ is divisible by $p^k$ and $A_k$ is an approximation to $\sqrt{-1}$ correct ($p$-adic sense) to $k$ places. Similarly the $B_k$ sequence gives the complement:

$$\cdots 13042214120132 33. = -\sqrt{-1}. \tag{17}$$

The point of this review is to indicate, first, that the degeneracy $B_5 = B_6 = 1068$ mentioned above (9) is associated with the last zero digit in (17). That is, $B_5 = 13233$ (quinary) and so is $B_6$. Similarly from the zero digits of (16) we find that $A_9 = A_8$ and $A_{13} = A_{12}$. Since an irrational $p$-adic cannot have periodic digits, [10, p. 196], it is reasonable to conjecture that the digits are "normal." This would imply that degenerates appear infinitely often in every $A_k$ and $B_k$ sequence for every $p$, and further that we should expect *multiple* degenerates, $A_k = A_{k+1} = A_{k+2}$, etc. For all that, aside from the $B_5 = B_6 = 1068$ for $p = 5$ and the $A_3 = A_4 = 239$ for $p = 13$ already mentioned, there are no other degenerates $\leqq 180{,}000$.

**8. The Difficulty of the Unsettled Questions.** It has often been remarked that questions like (13) are "very difficult." The intent of this section is to assess this difficulty. We do this by comparing the very simple Eratosthenes sieve for the ordinary prime sequence with the present one for $n^2 + 1$ and note that the latter is more complicated in the following three ways:

1.) Instead of *one* linear form, $mp$, for each prime, we have a double infinity: $A_k + mp^k$, $B_k + mp^k$.

2.) Instead of a zero origin we have $A_k$ and $B_k$ origins, which are not related to $p$ in any simple fashion. While $A_2$, $A_3$, $\cdots$ and $B_1$, $B_2$, $\cdots$ can be computed by the more or less complicated relations (2) through (6), $A_1$ can arise at any $n$ satisfying $\sqrt{p - 1} \leqq n \leqq (p - 1)/2$. Further, we have the complications of occasional degeneracy.

3.) Finally, whereas in the Eratosthenes sieve it is not necessary to divide, but it suffices to scratch the cells in the linear form, here we *must* divide the $p$ out. Otherwise, we would not obtain the new prime hidden in each $A_1^2 + 1$ which is not itself prime.

**9. Generalization.** In conclusion, it should be stated that while we have confined ourselves here to $n^2 + 1$ the same type of sieve method is applicable to $n^2 + a$, for $a = \pm 2, \pm 3$, etc. The main change is that these programs would be based on the $p$-adic square roots of $-a$ The sieve itself would generate those primes for which $-a$ is a quadratic residue, that is, all possible divisors. It is thought that comparable statistics will be found for the primes of these forms and for the "generalized irreducibles," that is, those $n$ which yield a new prime factor. This is now being investigated, [11].

Applied Mathematics Laboratory,
David Taylor Model Basin,
Washington, District of Columbia

1. L. E. Dickson, *History of the Theory of Numbers*, Stechert, New York, 1934, v. 1, Ch. XVI. For example, Euler (1752) gave $P(1500) = 161$. See also D. H. Lehmer, *Guide to Tables in the Theory of Numbers*, National Research Council, Washington, D. C., 1941, p. 31–32 and p. 45.

2. The most extensive table of all the prime factors of $n^2 + 1$ (up to $n = 31{,}622$) is the unpublished table of J. W. Wrench, Jr. See UMT 1, *MTAC*, v. I, 1943, p. 26. Recently a 704 program by the author in collaboration with Dr. Wrench raised this limit to 50,000 for a table of the *greatest* prime factor. However, we now consider that type of program (with trial divisions) to be superseded by the present sieve method.

3. G. H. Hardy & J. E. Littlewood, "Partitio numerorum III: On the expression of a number as a sum of primes," *Acta Math.*, v. XLIV, 1923, p. 48.

4. A. E. Western, "Note on the number of primes of the form $n^2 + 1$," Cambridge Phil. Soc., *Proc.*, v. XXI, 1922, p. 108–109. Western assumes $P(15000) = 1199$ following Cunningham, who omits $2 = 1^2 + 1$. The correct value of $P(15000)$ is 1200.

5. *Fortune*, June, 1958, p. 140.

6. John Todd, "A problem on arc tangent relations," *American Math Monthly*, v. LVI, 1949, p. 517–528.

7. S. D. Chowla & J. Todd, "The density of reducible integers," *Canadian Jour. of Math*, v. I, 1949, p. 297–299. The table of $R(N)$ to $N = 5000$ has many errors. It indicates $R(5000) = 1453$. A mimeographed errata sheet later circulated stated $R(5000) = 1458$, but the correct value is 1467.

8. John Todd, *Table of Arctangents of Rational Numbers*, NBS, Applied Math. Series 11, Washington, D. C., 1951.

9. While $\pi_+(N)$ and $\pi_-(N)$ are asymptotically equal, $\pi_-(N)$ is larger for about 99.6 per cent of the $N$ less than $10^6$. See a forthcoming paper of the author, "Quadratic residues and the distribution of primes," for the statistics of this and related phenomena. That this weakness of $\pi_+(N)$ will tend to raise $P(N)$ and lower $R(N)$ seems clear, but no serious attempt has been made to evaluate its effectiveness.

10. C. C. MacDuffee, *An Introduction to Abstract Algebra*, Wiley, New York, 1940, p. 193–202.

11. *Note added in proof, May 7, 1959.* The number of primes of the forms $n^2 + 2$, $n^2 - 2$, $n^2 + 3$, and $n^2 - 3$ up to $n = 180{,}000$ are 5847, 15134, 9240, and 11354, respectively. These numbers are all in good agreement with Conjecture F, [3], of Hardy and Littlewood. Fuller details will be published later.